Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/14

Sony FeliCa Contactless Smart Card IC Chip RC-S960/1

Paris, le 28 juin 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

DCSSI-2007/14

Nom du produit

Sony FeliCa Contactless Smart Card IC Chip RC-S960/1

Référence/version du produit

RC-S960/1

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4

Développeurs

Sony Corporation

4-7-35 Kitashinagawa Shinagawa-ku, Tokyo, 140-0001, Japan

Fujitsu

1-1 Kamikodanaka 4_Chome, Nakahara-Ku, Kawasaki 211-8588 Japan

Commanditaire

Sony Corporation

4-7-35 Kitashinagawa Shinagawa-ku, Tokyo, 140-0001, Japan

Centre d'évaluation

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 62 88 28 01, mél : ceaci@cnes.fr

Accords de reconnaissance applicables

CCRA

SOG-IS

IT Security Certified

Le produit est reconnu au niveau EAL4

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué « Sony FeliCa Contactless Smart Card IC Chip RC-S960/1 » est une carte à puce sans contact développée par Sony Corporation. Elle est destinée à être utilisée dans de nombreux domaines, notamment la finance.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par les éléments suivants :

- Nom commercial : IC Chip RC-S960/1
- Référence du logiciel : FeliCa OS version 3.31
- Référence de la ROM du produit : 0F sans aucun patch.
- Référence du microcontrôleur : CXD9861/MB94RS402, FR00 001
- Références des logiciels dédiés au microcontrôleur :
    - HAL-API version 22.0
    - DRNG Library version 22.0

Ces informations peuvent être vérifiées grâce aux commandes décrites dans les guides (cf. [guides]).

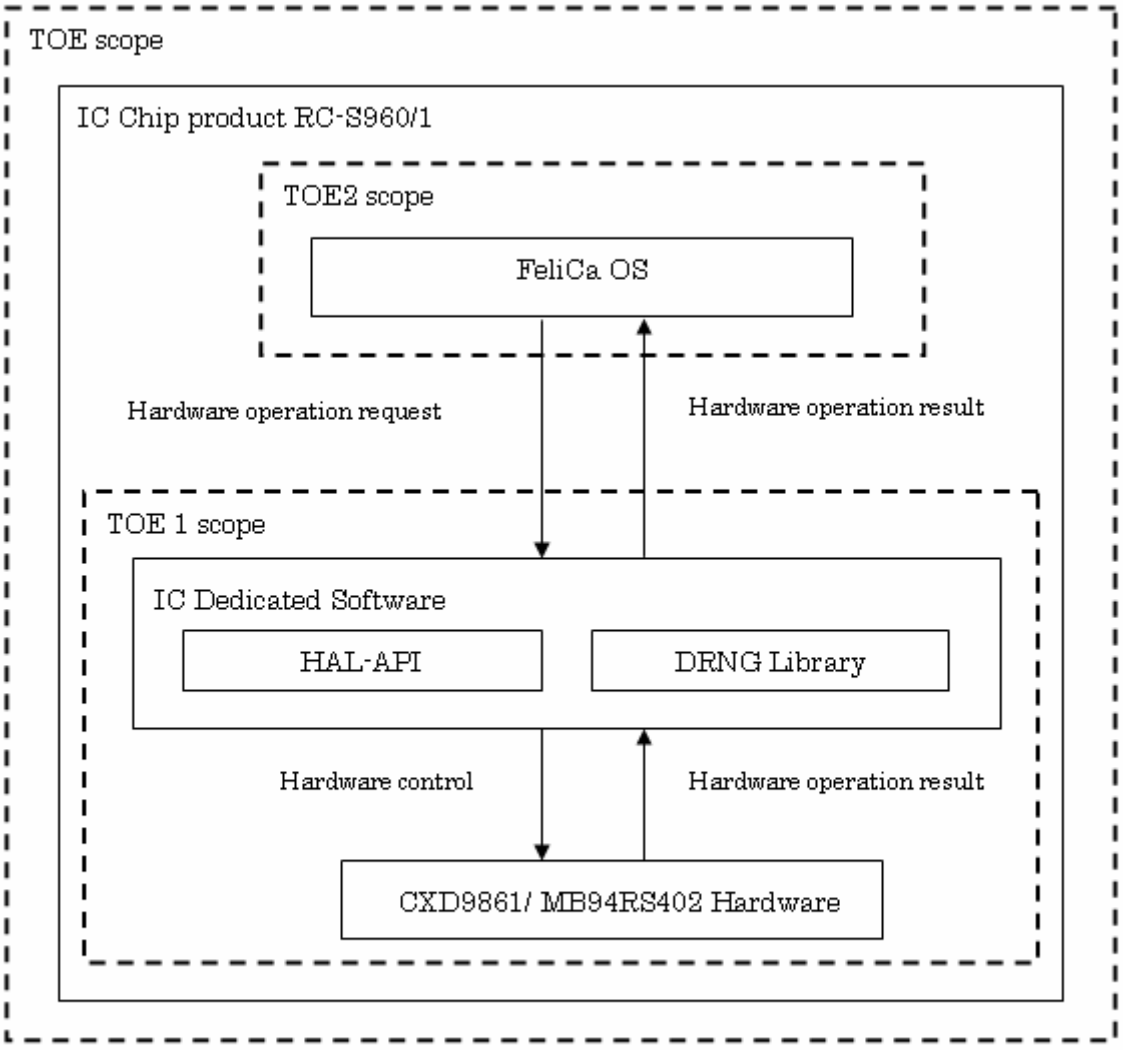
1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- La protection en confidentialité et en intégrité des données du client ;
- Le contrôle de flux sur les données de communication envoyées et reçues entre le produit et le lecteur/enregistreur ;
- La création et gestion du système de fichiers en mémoire FRAM ;
- Le contrôle d'accès aux fichiers pour l'enregistrement/ la lecture/ l'écriture et la suppression des fichiers en mémoire FRAM.

1.2.3. Architecture

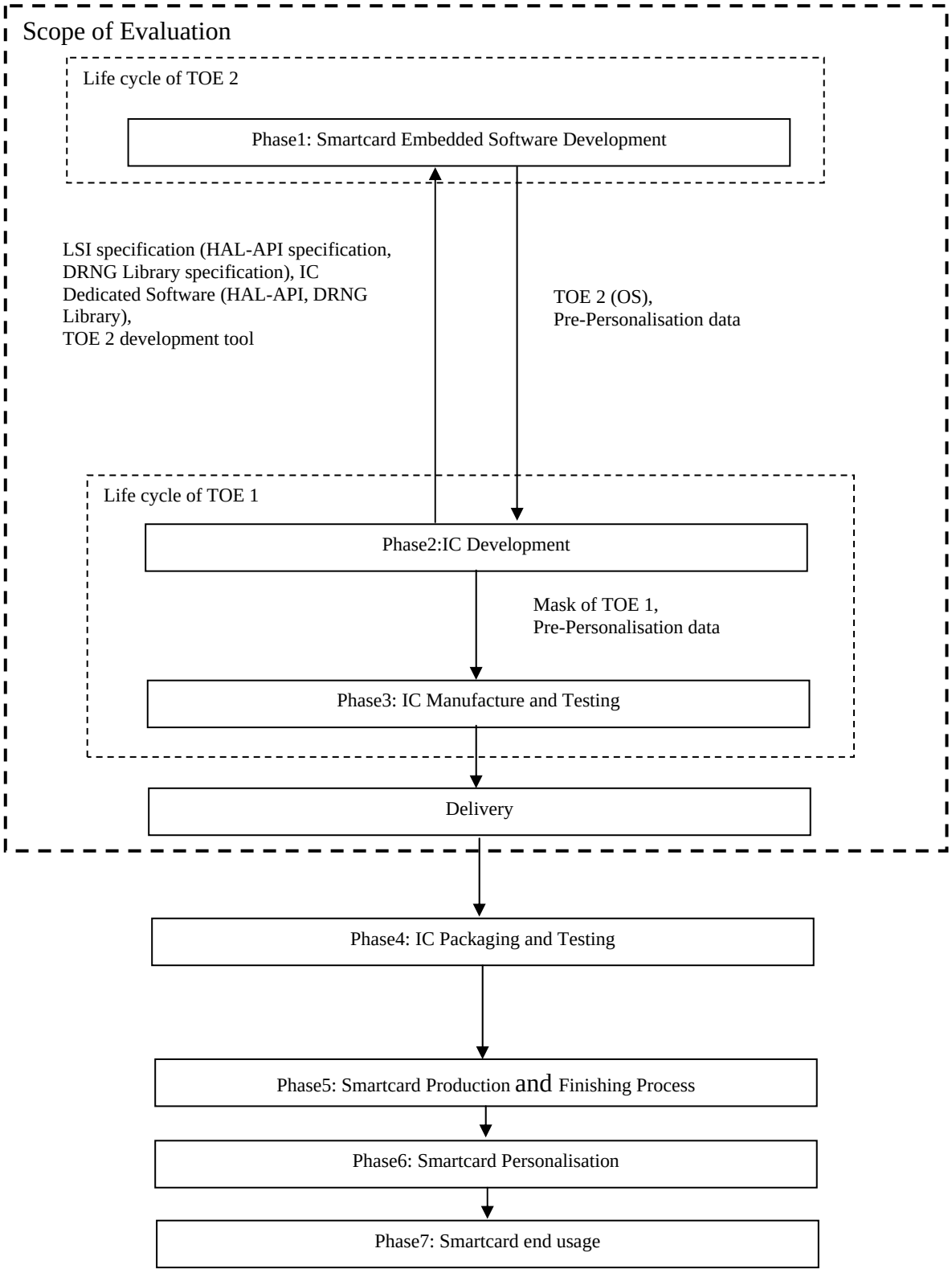
Le produit évalué est constitué d'un microcontrôleur et d'éléments logiciels dédiés sur lesquels est embarqué le système d'exploitation FeliCa OS.
Dans les schémas suivants le microcontrôleur et ses éléments logiciels dédiés seront identifiés par TOE1 et le système d'exploitation par TOE2. La cible d'évaluation correspond aux éléments identifiés par TOE1 et TOE2.



HAL: Hardware Abstraction Layer
DRNG: Deterministic Random Number Generator

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants :

Sony Gotenyama Garden office

4-7-35 Kitashinagawa Shinagawa-ku,
Tokyo, 140-0001
Japan

Sony Toyosato Plant

130 Koguchimae, Toyosato-cho, Tome-shi,
Miyagi-ken. 987-0362
Japan

Pour l'évaluation, l'évaluateur a considéré le fabricant de microcircuit, le développeur du masque logiciel et la fabricant de carte (« IC Manufacturer », « Mask developper » et « Card Manufacturer » dans la cible de sécurité) comme administrateur du produit et les rôles émetteur de carte, « administrateur de zone » et utilisateur de service (« Card Issuer », « Area Administrator » et « Service User » dans la cible de sécurité) comme « utilisateur du produit » tel qu'indiqué dans la cible de sécurité [ST].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, le guide [CCAP] a été appliqué.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur Fujitsu «CXD9861/ MB94RS402 with HAL-API & DRNG Library » au niveau EAL4 augmenté des composants ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4, conforme au profil de protection « Smartcard IC Platform Protection Profile » [PP0002]. Ce microcontrôleur a été certifié le 14 décembre 2006 sous la référence 2006/29.

Cette évaluation a aussi tenu compte de la maintenance du microcontrôleur du 23 avril 2007 sous la référence M-2007/03.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 15 juin 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

3. La certification

3.1. Conclusion

L'évaluation, identifiée au chapitre 2 et décrite dans le rapport technique d'évaluation [RTE], a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises par un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit «Sony FeliCa Contactless Smart Card IC Chip RC-S960/1» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 .

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- pour communiquer avec la carte de façon sécurisée, les produits TI devront fournir un canal de confiance ;

- des procédures de sécurité garantissant la confidentialité et l'intégrité de la cible d'évaluation et de ses données de fabrication et de test devront être appliquées après la livraison de la cible d'évaluation et jusqu'à l'utilisateur final (cf.1.2.4). Ces mesures de sécurité ont pour but de prévenir les risques liés à la copie, la modification, la rétention, le vol ou l'utilisation non autorisée de la cible d'évaluation.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CC RA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, la Corée du Sud, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Nouvelle-Zélande, la Norvège, les Pays-Bas, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1**	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - RC-S960/1 Composite Security Target v1.43 réf. : 960-ST-E01-43 Pour les besoins de publication la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - RC-S960/1 Composite Security Target - Public Version réf. :960-STL-E01-43
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - Project: TYPHON23 réf. : TYP_ETR v5.0 du 15/06/07 - Addendum of Evaluation Technical Report Project: TYPHON23 réf. : TYP_ADD_ETR revision 1.0 26/06/07
[CONF]	RC-S960 Configuration Management List 1 00 réf. : 960-CML-E01-00 /1.00
[GUIDES]	Guide de livraison du produit : - IC Delivery Rules v1.2 réf. : 960-DEL_IC-E01-20 - Document Delivery Rules v1.0 réf.: 960-DEL_DOC-E01-00 Guides d'utilisation et d'administration du produit : - FeliCa Card IC Security Operation Guidelines v1.0 réf. : M292-E0.1-00 - RC-S960 Series FeliCa OS Command Reference Manual v1.0 réf. : M247-E01-00 - Security Reference Manual Group Service Key & User Service Key Generation v1.0 réf. : SR-030-001E - Security Reference Manual Mutual Authentication & Packet Cryptography v1.0 réf. : SR-030-002E - Security Reference Manual Issuing Package Generation v1.0 réf. : SR-030-003E - Security Reference Manual Changing Key Package Generation v1.0 réf. : SR-030-004E Guide d'administration du produit : - RC-S960 Series Manufacture ID Writing Procedure v1.0 réf. : M248-E01-00 - RC-S960 Series Inspection/Verification Procedure v1.0 réf. : M252-E01-00 - FeliCa Card Rewriting Transport key v1.1 réf. : Tec01-E01-10 - RC-S960 Series FeliCa OS Status Flag Reference v 1.0

	réf. : M294-E01-00
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI sous la référence BSI-PP-0002-2001.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.